

# United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

## APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

[REDACTED], Bear, Delaware, described  
more particularly on Attachment A

CASE NUMBER: 05-96M-MPT

**REDACTED**

I, Anthony H. Crabtree

being duly sworn deposes and says:

I am a(n) Special Agent, FBI

Official Title

and have reason to believe

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

[REDACTED], Bear, DE, described more particularly above

in the \_\_\_\_\_ District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

see Attachment B

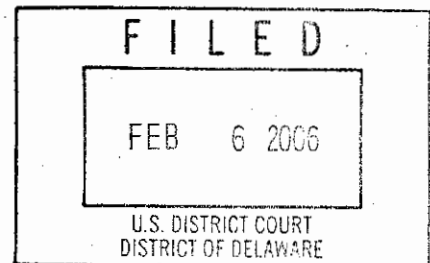
which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

contraband and evidence of a crime

concerning a violation of Title 18 United States code, Section(s) 2252

The facts to support a finding of Probable Cause are as follows:

see attached affidavit



Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

SA Anthony H. Crabtree  
Signature of Affiant

SA Anthony H. Crabtree, FBI

Sworn to before me, and subscribed in my presence

July 1, 2005

Honorable Gregory M. Sleet  
United States District Court

Name and Title of Judicial Officer

at Wilmington, Delaware  
City and State

[Signature]  
Signature of Judicial Officer

ATTACHMENT A

The location [REDACTED] Bear, Delaware is an apartment located on the first floor of building [REDACTED] of the [REDACTED] [REDACTED] It has a green front door with the numbers [REDACTED] displayed on the front.

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

1. Computer(s), computer hardware, computer software to include but not limited to Peer 2 Peer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes pertaining

to the possession, receipt, or distribution of child pornography as defined in 18 U.S. C. § 2256(8) or to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S. C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica, including but not limited to the following computer files:

a. PTHC Childlover P050.jpg (Image depicts a female child, approximately 10 years old sitting in a chair exposing her genital area in a lascivious manor).

b. PTHC Childlover P035.jpg (Image depicts a female child, approximately 10 years old on her knees without any clothes on exposing her genital area in a lascivious manor).

c. PTCH Childlover P003.jpg (Image depicts a female child, approximately 11 years old performing oral sex on a male individual).

d. PTHC Childlover P036.jpg (Image depicts a female child, approximately 10 years old lying on a bed without and cloths on exposing her genital area in a lascivious manor).

e. PTHC Childlover P037.jpg (Image depicts a female

child, approximately 10 years old lying on a bed without and cloths on exposing her genital area in a lascivious manor).

f. PTHC Childlover P049.jpg (Image depicts a female child, approximately 10 years old sitting in a chair exposing her genital area in a lascivious manor).

g. PTHC Childlover P038.jpg (Image depicts a female child, approximately 10 years old lying on a bed fully dressed with her legs spread apart).

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or

correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters papers, e-mail messages, chat logs and

electronic messages, and other digital data files) that concern accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors that may be connected to other visual depictions of minors engaging in sexual explicit conduct.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase,



sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

16. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

17. Any and all indicia of possession and use of the computer located at 1422 Elk Way, Newark, Delaware, (including, but not limited to, Internet Provider subscriber records including but not limited to Comcast Communication Internet Services, correspondence, e-mail messages, email headers, email accounts information, chat logs, screen names, buddy lists, electronic messages, web cache information,



employment records, rental or lease agreements, and rental or lease payments).

THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF DELAWARE

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Anthony H. Crabtree, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Baltimore Division, Wilmington, Delaware Resident Agency, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since December 1, 2002, and am currently assigned to the Baltimore Division, Wilmington, Delaware Resident Agency. Since joining the FBI, I have been involved in the investigation of violent crimes, white collar crimes, and terrorism activity. Since January 2004, I have been assigned to investigate Crimes Against Children that include Sexual Exploitation of Children (SEOC) violations of federal law. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended FBI Crimes Against Children Training as well as

training in the Innocent Images National Initiative Undercover Internet Training.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of a computer having internet connection with a service and billing address of 1422 Elk Way, Bear, Delaware 19701. As will be shown below, there is probable cause to believed that someone using a computer at the above listed address has received, possessed, and/or transmitted child pornography, in violation of Title 18, United States Code, Section 2252. I am submitting this Affidavit in support of a search warrant authorizing a search of the residence located at [REDACTED], Bear, Delaware 19701, ( the "Premises"), for the items specified in Attachment B hereto. Said Premises is more particularly described below. I am requesting authority to search the entire Premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits and evidence of crime.

4. All information contained in this affidavit is

either personally known to the affiant or has been related to the affiant by other Special Agents of the Federal Bureau of Investigation. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2252, are presently located at [REDACTED], Bear, Delaware 19701.

STATUTORY AUTHORITY

5. This investigation concerns alleged violation of Title 18, United States Code, Sections 2252, relating to material involving the sexual exploitation of minors. 18 U.S.C. Section 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed, shipped or transported in interstate or foreign commerce by any means, including by computer, when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. Section 2256(8) which reads in part, any visual "... depiction ... of sexually explicit conduct where ... the production of the visual depiction involves the use of a minor engaged in sexually explicit conduct ...."

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. Section 2256(5).

d. "Sexually explicit conduct," means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of

the genitals or pubic area of any persons. See 18 U.S.C.

Section 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskette, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital

information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operated systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords and data security devices, " as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it



inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address," refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. The term "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means. Whether in handmade form (including, but not limited to, writing, drawings, and paintings) photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photograph records, printing, and typing), or electrical, electronic or magnetic form (including, but not limited to , tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart

cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTER AND CHILD PORNOGRAPHY

7. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secured storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailing and telephone calls.

8. The development of computers has changed the production and distribution of child pornography. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet and the World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing

service that provide e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such

information is often maintained indefinitely until overwritten by other data.

14. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Shareaza, one type of P2P software, sets up its searches by keyword (among other criterion). The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

15. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her

computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Shareaza user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Shareaza user downloading an image file receives the entire image from one computer.

17. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address

provides a unique location making it possible for data to be transferred between computers.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

18. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence



is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been

used to create the data (whether stored on hard drives or on external media.)

20. Finally, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

21. Affiant has been informed that FBI Supervisory Special Agent (SSA) James T. Clemente has worked in the Behavioral Analysis Unit of the FBI since 1998. SSA Clemente has been a Special Agent with the FBI since 1987. As a member of the Behavioral Analysis Unit, SSA Clemente consults on child exploitation cases throughout the United States, South America, and certain European and African countries. Since 1998, he has received three Exceptional Performance Awards from the Department of Justice and a Superior Service Award from the FBI. In addition, he has received numerous letters of commendation from state, federal, and local law enforcement in connection with his work in the Behavioral Analysis Unit.

22. SSA Clemente's training has involved a significant number of specialized courses in the area of child

exploitation, including, but not limited to the following: Innocent Images On-Line Sex Crimes Against Children; National Crimes Against Children; On-Line Sex Crimes Against Children; Clinical Forensic Psychology; Behavioral Analysis of Violent Crime; Missing and Exploited Children Seminar; Research Methodologies; MO, Ritual & Signature Advanced Seminar; and Criminology. In addition, he has mentored under, worked with, studied the articles of, and taught with Kenneth V. Lanning, a Supervisory Special Agent, FBI (retired as of October, 2000). SSA Lanning has over the past 27 years authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work forms the basis of the behavioral analysis performed by the FBI in child exploitation cases.

23. SSA Clemente has assisted in the writing of numerous search warrant affidavits and has testified as an expert witness in federal court in the areas of child sex offender behavior, child sexual victimology and child pornography. He has given over 100 presentations and lectures to local, state and federal law enforcement agencies, prosecutors, and health care professional throughout the United States on various topics related to child exploitation, including, but not limited to the following topics: Behavioral Analysis of Child

Sex Crimes Offenders, On-Line Sex Crimes Against Children, and Equivocal Death Investigations.

24. As a member of the Behavioral Analysis Unit, SSA Clemente has analyzed and consulted on between one and two hundred child sexual exploitation and victimization cases a year. His analyses are based on all available evidence, including chat records, image collection analysis, collection themes, possession of erotica, possession of sexual paraphernalia, fantasy literature and writings, other relevant acts, and background information. The vast majority of the cases he has analyzed have involved either Preferential or Situational Sex Offenders. His role in these cases has varied as follows: analyzing investigative results for the purpose of making investigative suggestions, providing interview strategies for subjects and victims, and consulting with local, state and federal prosecutors on trial strategies. In addition, SSA Clemente has interviewed between 80 and 100 offenders himself. A behavioral assessment is not a clinical diagnosis; rather, it is a law enforcement tool used to identify and predict offender behavior.

25. SSA Clemente has advised agents with the FBI of the following traits and characteristics that are generally found to exist and be true in cases involving individuals who

collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such

individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.


e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child

pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

#### BACKGROUND OF THE INVESTIGATION

26. On March 23, 2005, Special Agents of the Buffalo Division of the FBI, using an internet connected computer, conducted an undercover session and downloaded child pornography from the user of the Shareaza P2P software. Special Agents conducted a keyword search using the term "pthc" which is known to be associated with a series of images of child sexual abuse. Agents viewed the results of the search and observed multiple files available to be viewed and downloaded by others at the Internet Protocol (IP) Address

. The files downloaded during the undercover operation had the following names and are briefly described by your Affiant:

a. PTHC Childlover P050.jpg (Image depicting a female child, approximately 10 years old, sitting in a chair exposing her genital area in a lascivious manor).

b. PTHC Childlover P035.jpg (Image depicting a female child, approximately 10 years old, on her knees without any clothes on exposing her genital area in a lascivious



manor).

c. PTCH Childlover P003.jpg (Image depicting a female child, approximately 11 years old, performing oral sex on a male individual).

d. PTHC Childlover P036.jpg (Image depicting a female child, approximately 10 years old, lying on a bed without any cloths on exposing her genital area in a lascivious manor).

e. PTHC Childlover P037.jpg (Image depicting a female child, approximately 10 years old, lying on a bed without any cloths on exposing her genital area in a lascivious manor).

f. PTHC Childlover P049.jpg (Image depicting a female child, approximately 10 years old, sitting in a chair exposing her genital area in a lascivious manor).

g. PTHC Childlover P038.jpg (Image depicting a female child, approximately 10 years old, lying on a bed fully dressed with her legs spread apart).

27. A search of the American Registry for Internet Numbers (ARIN) online database indicated that the IP address [REDACTED] is registered to the Internet Service Provider Comcast Cable Communication, Inc. According to ARIN's website, ARIN is described as a nonprofit organization

responsible for managing the Internet numbering resources for North America, a portion of the Caribbean, and sub-equatorial Africa. Results from an administrative subpoena sent to Comcast Cable Communication, Inc. for the date and time the images were downloaded, revealed that the IP address was assigned to the account number subscriber listed as Dennis Diehl, [REDACTED] PA 19061 (the Comcast Diehl account). The results further revealed that the Comcast Diehl account was logged on during the time of the undercover operation between 12:01 p.m. EST. and 12:13 p.m. EST on March 23, 2005.

28. a. Comcast IP Services, LLC reported that on April 30, 2005, Dennis Diehl canceled his high speed internet service that had a service address of [REDACTED], Marcus Hook PA 19061. Furthermore, Comcast reported that on the same date Dennis Deal subscribed to Comcast high speed internet service with a service address of [REDACTED] Bear, Delaware 19701.

b. The FBI has searched various record databases for information about Dennis Diehl. Pennsylvania Bureau of Motor Vehicles' records indicate that Dennis Diehl has a social security number [REDACTED] and date of birth [REDACTED]

c. On June 22, 2005, a request was issued to the United States Postal Inspection Service, requesting mailing information for 1422 Elk Way, Bear, Delaware 19701. The results of the request verified that mail is now being delivered to Dennis Diehl at [REDACTED] Bear, Delaware 19701.

d. On June 30, 2005, your affiant conducted physical surveillance of the apartment located at [REDACTED] Bear, Delaware. Your affiant identified and observed Dennis Diehl exit the apartment and leave in a 2002 Ford pick-up truck, with a Pennsylvania tag number [REDACTED]. The vehicle is registered in Pennsylvania to Dennis Diehl.

29. On June 27, 2005, Affiant observed the residence located at [REDACTED] Bear, Delaware, and it is accurately described below.

DESCRIPTION OF THE PREMISES TO BE SEARCHED

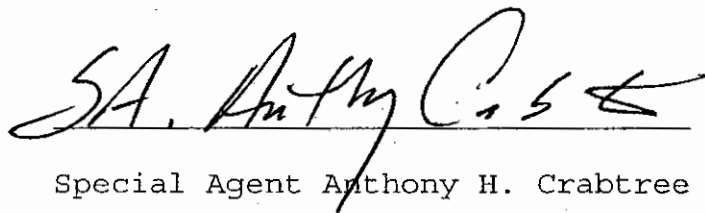
30. The location [REDACTED], Bear, Delaware is an apartment located on the first floor of building [REDACTED]. It has a green front door with the numbers [REDACTED] displayed on the front.

CONCLUSION

31. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause

to believe that an individual who resides at the residence described above is involved in possession, receiving and transmitting child pornography. Your affiant respectfully submits that there is probable cause to believe that an individual with access to the computer located in the residence described above has violated 18 U.S.C. §§ 2252. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violation of 18 U.S.C. §§ 2252, is located in the residence described above, and this evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

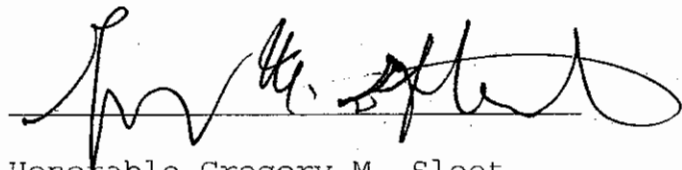
32. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

A handwritten signature in dark ink, appearing to read "SA. Anthony H. Crabtree", is written over a horizontal line.

Special Agent Anthony H. Crabtree  
Federal Bureau of Investigation

Sworn and subscribed before me

this \_\_\_\_\_ day of

A handwritten signature in black ink, appearing to read "Gregory M. Sleet", written over a horizontal line.

Honorable Gregory M. Sleet

United States District Court